

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-318330

(P2004-318330A)

(43) 公開日 平成16年11月11日(2004. 11. 11)

(51) Int. Cl. <sup>7</sup>

F I

テーマコード (参考)

G06F 11/00

G06F 9/06 630A

5B017

G06F 1/00

G06F 12/14 320A

5B076

G06F 9/445

G06F 9/06 640A

G06F 12/14

G06F 9/06 660L

審査請求 未請求 請求項の数 11 O L (全 13 頁)

(21) 出願番号 特願2003-109170 (P2003-109170)

(22) 出願日 平成15年4月14日 (2003. 4. 14)

(71) 出願人 503121103

株式会社ルネサステクノロジ

東京都千代田区丸の内二丁目4番1号

(74) 代理人 100080001

弁理士 筒井 大和

(72) 発明者 飯島 雅人

東京都千代田区丸の内二丁目4番1号 株

式会社ルネサステクノロジ内

(72) 発明者 浅井 俊雄

東京都千代田区丸の内二丁目4番1号 株

式会社ルネサステクノロジ内

Fターム (参考) 5B017 AA03 BA04 CA12 CA16

5B076 BB06 EB03

(54) 【発明の名称】 半導体集積回路装置およびデータ処理システム

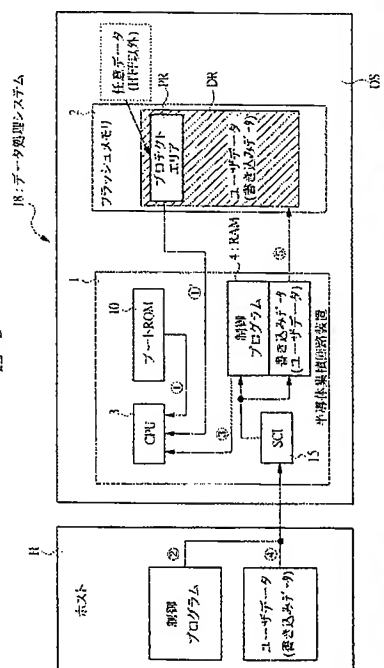
(57) 【要約】

【課題】 外付けで不揮発性メモリが接続可能な半導体集積回路装置において、ユーザデータの書き込み後の該ユーザデータの漏洩を防止する。

【解決手段】 リセット後、半導体集積回路装置1がブートモードに移移すると、CPU3がブートROM10からフラッシュメモリ2の制御プログラムをダウンロードするためのブートプログラムを読み出す。続いて、ホストHとのビットレートの合わせ込みを行い、CPU3はフラッシュメモリ2のプロテクトエリアPRに書き込まれているプロテクトデータを参照し、該プロテクトデータがプロテクト状態となっているか、否かを判断する。このとき、プロテクトデータがプロテクト状態となっている際には、半導体集積回路装置1は、スタンバイ状態（あるいは、スリープ状態、無限ループ）となり、制御プログラムのダウンロードが一切実行できなくなる。

【選択図】 図2

図 2



## 【特許請求の範囲】

## 【請求項1】

外付けで不揮発性メモリが接続可能で、前記不揮発性メモリを制御する制御プログラムをダウンロードするブートプログラムが格納された半導体集積回路装置であって、  
前記ブートプログラムに基づいて、前記制御プログラムをダウンロードする制御部を備え、  
前記制御部は、  
ブートモードによる起動時において、プロテクトデータに応じて第1、または第2の状態のいずれであるかを判断し、前記第1の状態の際には、前記制御プログラムのダウンロードを実行し、前記第2の状態の際には、前記制御プログラムのダウンロードを実行しないことを特徴とする半導体集積回路装置。

## 【請求項2】

外付けで不揮発性メモリが接続可能で、前記不揮発性メモリを制御する制御プログラムをダウンロードするブートプログラムが格納された半導体集積回路装置であって、  
前記ブートプログラムが格納されたブートプログラム格納用メモリと、  
前記制御プログラムを格納する揮発性メモリと、  
前記ブートプログラムに基づいて、前記制御プログラムのダウンロード、および前記制御プログラムに基づく前記不揮発性メモリの動作制御を行う制御部とを備え、  
前記制御部は、ブートモードによる起動時において、プロテクトデータに応じて第1、または第2の状態のいずれであるかを判断し、前記第1の状態の際には、前記制御プログラムのダウンロードを実行し、前記第2の状態の際には、前記制御プログラムのダウンロードを実行しないことを特徴とする半導体集積回路装置。

## 【請求項3】

外付けで不揮発性メモリが接続可能で、前記不揮発性メモリを制御する制御プログラムをダウンロードするブートプログラムが格納された半導体集積回路装置であって、  
前記ブートプログラム、および前記不揮発性メモリに格納されたユーザデータの読み出し動作を制御する通常動作制御プログラムをダウンロードする通常動作ブートプログラムがそれぞれ格納されたブートプログラム格納用メモリと、  
前記制御プログラム、または通常動作制御プログラムを格納する揮発性メモリと、  
前記ブートプログラムに基づく前記制御プログラムのダウンロード、前記通常動作ブートプログラムに基づく前記通常動作制御プログラムのダウンロード、および前記制御プログラム、または前記通常動作制御プログラムのいずれかに基づく前記不揮発性メモリの動作制御を行う制御部とを備え、  
前記制御部は、ブートモードによる起動時において、プロテクトデータに応じて第1、または第2の状態のいずれであるかを判断し、前記第1の状態の際には、前記制御プログラムのダウンロードを実行し、前記第2の状態の際には、前記制御プログラムのダウンロードを実行しないことを特徴とする半導体集積回路装置。

## 【請求項4】

請求項1～3のいずれか1項に記載の半導体集積回路装置において、前記制御部は、前記制御プログラムをダウンロードする前に、前記プロテクトデータを読み出し、第1、または第2の状態のいずれであるかを判断することを特徴とする半導体集積回路装置。

## 【請求項5】

請求項4記載の半導体集積回路装置において、前記制御部は、前記第1の状態によって前記制御プログラムのダウンロードを実行した際に、前記不揮発性メモリのデータ領域に前記第2の状態となるプロテクトデータに書き換えることを特徴とする半導体集積回路装置。

## 【請求項6】

請求項1～5のいずれか1項に記載の半導体集積回路装置において、初期化終了後に、前記ブートモードを設定するブートモード設定用外部端子を有することを特徴とする半導体集積回路装置。

## 【請求項7】

ユーザデータが格納される不揮発性メモリと前記不揮発性メモリが外付けで接続可能な半導体集積回路装置とを有するデータ処理装置と、前記データ処理装置を管理する情報処理装置とよりなるデータ処理システムであって、

前記半導体集積回路装置は、

前記不揮発性メモリを制御する制御プログラムをダウンロードするブートプログラムが格納されたブートプログラム格納用メモリと、

前記制御プログラムを格納する揮発性メモリと、

前記ブートプログラムに基づいて、前記制御プログラムのダウンロード、および前記制御プログラムに基づく前記不揮発性メモリの動作制御を行う制御部とを備え、

前記不揮発性メモリは、第1、または第2の状態のいずれかの状態を設定するプロテクトデータが格納されるデータ領域を有し、

前記制御部は、ブートモードによる起動時において、前記不揮発性メモリのデータ領域に格納されたプロテクトデータを読み出し、第1、または第2の状態のいずれであるかを判断し、前記第1の状態の際には、前記情報処理装置からの前記制御プログラムのダウンロードを実行し、前記第2の状態の際には、前記制御プログラムのダウンロードを実行しないことを特徴とするデータ処理システム。

## 【請求項8】

ユーザデータが格納される不揮発性メモリと前記不揮発性メモリが外付けで接続可能な半導体集積回路装置とを有するデータ処理装置と、前記データ処理装置を管理する情報処理装置とよりなるデータ処理システムであって、

前記半導体集積回路装置は、

前記不揮発性メモリを制御する制御プログラムをダウンロードするブートプログラム、および前記不揮発性メモリに格納されたユーザデータの読み出し動作を制御する通常動作制御プログラムをダウンロードする通常動作ブートプログラムがそれぞれ格納されたブートプログラム格納用メモリと、

前記制御プログラム、または前記通常動作制御プログラムを格納する揮発性メモリと、

前記ブートプログラムに基づく前記制御プログラムのダウンロード、前記通常動作ブートプログラムに基づく前記通常動作制御プログラムのダウンロード、および前記制御プログラム、または前記通常動作制御プログラムのいずれかに基づく前記不揮発性メモリの動作制御を行う制御部とを備え、

前記制御部は、ブートモードによる起動時において、前記不揮発性メモリに格納されたプロテクトデータに応じて第1、または第2の状態のいずれであるかを判断し、前記第1の状態の際には、前記制御プログラムのダウンロードを実行し、前記第2の状態の際には、前記制御プログラムのダウンロードを実行しないことを特徴とするデータ処理システム。

## 【請求項9】

請求項7または8記載のデータ処理システムにおいて、前記制御部は、前記第1の状態により、前記情報処理装置からの前記制御プログラムのダウンロードを実行した際に、前記不揮発性メモリのデータ領域に前記第2の状態となるプロテクトデータに書き換えることを特徴とするデータ処理システム。

## 【請求項10】

請求項7～9のいずれか1項に記載のデータ処理システムにおいて、前記制御部は、前記制御プログラムを前記情報処理装置からダウンロードする前に、前記プロテクトデータを読み出し、第1、または第2の状態のいずれであるかを判断することを特徴とするデータ処理システム。

## 【請求項11】

請求項7～10のいずれか1項に記載のデータ処理システムにおいて、前記半導体集積回路装置は、初期化終了後に、前記ブートモードを設定するブートモード設定用外部端子を有することを特徴とするデータ処理システム。

## 【発明の詳細な説明】

## 【0001】

## 【発明の属する技術分野】

本発明は、データのプロテクト技術に関し、特に、ブートプログラムを備えた半導体集積回路装置におけるデータプロテクトに適用して有効な技術に関するものである。

## 【0002】

## 【従来の技術】

フラッシュメモリなどの不揮発性メモリが備えられていない、いわゆる、ROM (Read Only Memory) レスマイクロコンピュータなどの半導体集積回路装置をデータ処理システムなどに実装する際には、該ROMレスマイクロコンピュータとともにフラッシュメモリをプリント配線基板などの実装基板に実装する場合がある。

## 【0003】

このROMレスマイクロコンピュータには、ブートプログラムが格納されている。このブートプログラムは、フラッシュメモリにアプリケーションプログラムなどのユーザデータを書き込むための書き込み制御プログラムをダウンロードするプログラムである。

## 【0004】

そして、ROMレスマイクロコンピュータは、ブートプログラムによりダウンロードした書き込み制御プログラムに基づいて、フラッシュメモリにユーザデータを書き込む。

## 【0005】

## 【発明が解決しようとする課題】

ところが、上記のような半導体集積回路装置におけるアプリケーションプログラムの書き込み技術では、次のような問題点があることが本発明者により見い出された。

## 【0006】

フラッシュメモリに書き込まれたユーザデータは、ROMレスマイクロコンピュータからのアクセスが可能であるが、該ユーザデータにフラッシュメモリの読み出し機能がなければ、該フラッシュメモリが実装基板に実装されている限り、第三者がユーザデータを読み出すことはできない。

## 【0007】

しかし、ROMレスマイクロコンピュータに格納されているブートプログラムを用いて、第三者が、書き込み制御プログラムの代わりに、フラッシュメモリの読み出し制御プログラムをダウンロードした場合、該ROMレスマイクロコンピュータを介して、フラッシュメモリに書き込まれたアプリケーションプログラムの内容が読み出されてしまう恐れがある。

## 【0008】

本発明の目的は、ユーザデータの書き込み後に、該ユーザデータの読み出しを防止するプロテクトをかけることにより、ユーザデータの漏洩を防止することのできる半導体集積回路装置およびデータ処理システムを提供することにある。

## 【0009】

本発明の前記ならびにその他の目的と新規な特徴は、本明細書の記述および添付図面から明らかになるであろう。

## 【0010】

## 【課題を解決するための手段】

本願において開示される発明のうち、代表的なものの概要を簡単に説明すれば、以下のとおりである。

## 【0011】

すなわち、本発明は、外付けでデータ書き換えが可能な不揮発性メモリが接続可能で、該不揮発性メモリを制御する制御プログラムをダウンロードするブートプログラムが格納された半導体集積回路装置であって、ブートプログラムに基づいて、制御プログラムをダウンロードする制御部を備え、該制御部は、ブートモードにおいて、プロテクトデータに応じて第1、または第2の状態のいずれであるかを判断し、第1の状態の際には制御プログラムのダウンロードを実行し、第2の状態では制御プログラムのダウンロードを実行しな

いものである。

【0012】

また、本願のその他の発明の概要を簡単に示す。

【0013】

また、本発明は、外付けで不揮発性メモリが接続可能で、該不揮発性メモリを制御する制御プログラムをダウンロードするブートプログラムが格納された半導体集積回路装置であって、ブートプログラムが格納されたブートプログラム格納用メモリと、制御プログラムを格納する揮発性メモリと、ブートプログラムに基づいて、制御プログラムのダウンロード、および制御プログラムに基づく不揮発性メモリの動作制御を行う制御部とを備え、制御部は、ブートモード時に、プロテクトデータに応じて第1、または第2の状態のいずれであるかを判断し、第1の状態の際には制御プログラムのダウンロードを実行し、第2の状態では、制御プログラムのダウンロードを実行しないものである。

【0014】

さらに、本発明は、外付けで不揮発性メモリが接続可能で、該不揮発性メモリを制御する制御プログラムをダウンロードするブートプログラムが格納された半導体集積回路装置であって、ブートプログラム、および不揮発性メモリに格納されたユーザデータの読み出し動作を制御する通常動作制御プログラムをダウンロードする通常動作ブートプログラムがそれぞれ格納されたブートプログラム格納用メモリと、制御プログラム、または通常動作制御プログラムを格納する揮発性メモリと、ブートプログラムに基づく制御プログラムのダウンロード、通常動作ブートプログラムに基づく通常動作制御プログラムのダウンロード、および制御プログラム、または通常動作制御プログラムのいずれかに基づく不揮発性メモリの動作制御を行う制御部とを備え、制御部は、ブートモードによる起動時において、不揮発性メモリに格納されたプロテクトデータに応じて第1、または第2の状態のいずれであるかを判断し、第1の状態の際には制御プログラムのダウンロードを実行し、第2の状態の際では制御プログラムのダウンロードを実行しないものである。

【0015】

ここで通常動作とは、該不揮発性メモリに格納される通常動作ブートプログラム、通常動作制御プログラム、ユーザーアプリケーションプログラム等のプログラムを実行する動作であり、半導体集積回路装置のリセット解除後、該通常動作ブートプログラムから実行がなされるものである。

【0016】

また、本発明は、ユーザデータが格納される不揮発性メモリと不揮発性メモリが外付けで接続可能な半導体集積回路装置とを有するデータ処理装置と、データ処理装置を管理する情報処理装置とよりなるデータ処理システムであって、半導体集積回路装置は、不揮発性メモリを制御する制御プログラムをダウンロードするブートプログラムが格納されたブートプログラム格納用メモリと、制御プログラムを格納する揮発性メモリと、ブートプログラムに基づいて、制御プログラムのダウンロード、および制御プログラムに基づく不揮発性メモリの動作制御を行う制御部とを備え、不揮発性メモリは、第1、または第2の状態のいずれかの状態を設定するプロテクトデータが格納されるデータ領域を有し、制御部は、ブートモードによる起動時において、不揮発性メモリのデータ領域に格納されたプロテクトデータを読み出し、第1、または第2の状態のいずれであるかを判断し、第1の状態の際には情報処理装置からの制御プログラムのダウンロードを実行し、第2の状態の際には制御プログラムのダウンロードを実行しないものである。

【0017】

さらに、本発明は、ユーザデータが格納される不揮発性メモリと該不揮発性メモリが外付けで接続可能な半導体集積回路装置とを有するデータ処理装置と、該データ処理装置を管理する情報処理装置とよりなるデータ処理システムであって、半導体集積回路装置は、不揮発性メモリを制御する制御プログラムをダウンロードするブートプログラム、および不揮発性メモリに格納されたユーザデータの読み出し動作を制御する通常動作制御プログラムをダウンロードする通常動作ブートプログラムがそれぞれ格納されたブートプログ

ラム格納用メモリと、制御プログラム、または通常動作制御プログラムを格納する揮発性メモリと、ブートプログラムに基づく制御プログラムのダウンロード、通常動作ブートプログラムに基づく通常動作制御プログラムのダウンロード、および制御プログラム、または通常動作制御プログラムのいずれかに基づく不揮発性メモリの動作制御を行う制御部とを備え、制御部は、ブートモードによる起動時において、プロテクトデータに応じて第1、または第2の状態のいずれであるかを判断し、第1の状態の際には制御プログラムのダウンロードを実行し、第2の状態の際には制御プログラムのダウンロードを実行しないものである。

【0018】

【発明の実施の形態】

以下、本発明の実施の形態を図面に基づいて詳細に説明する。

【0019】

図1は、本発明の一実施の形態による半導体集積回路装置のブロック図、図2は、図1の半導体集積回路装置を用いて構成したデータ処理システムのブロック図、図3は、図2の半導体集積回路装置の各動作モードに対応するフラッシュメモリの状態説明図、図4は、図2のデータ処理システムにおける動作フローチャート、図5は、図1の半導体集積回路装置における状態遷移図、図6は、図1の半導体集積回路装置における端子機能の説明図、図7は、図2のデータ処理システムにおける通信動作処理の流れを示す説明図である。

【0020】

本実施の形態において、半導体集積回路装置1は、たとえば、CD (Compact Disc) やDVD (Digital Versatile Disc) などの光ディスク媒体に記憶されている情報の再生などを行うディスクドライブ装置に設けられ、光ディスク媒体のドライブ制御などを行う。

【0021】

この半導体集積回路装置1は、フラッシュメモリなどの不揮発性メモリが内蔵されていない、いわゆる、ROMレスマイクロコンピュータからなる。この半導体集積回路装置1には、フラッシュメモリ (不揮発性メモリ) 2 (図2) が外部接続されている。

【0022】

半導体集積回路装置1は、図1に示すように、中央処理装置-(CPU: Central Processing Unit) 3、RAM (Random Access Memory) 4、データ転送ユニット5、割り込みコントローラ6、BSC (Bus State Controller) 7、周辺回路8、クロック発振器9、ブートROM (Read Only Memory) 10、およびI/O (Input/Output) ポートPなどから構成されている。

【0023】

CPU (制御部) 3は、外部からの所定の信号などによってフラッシュメモリ2に格納された情報を読み出し、所定の処理を行う。また、CPU3が処理を行うことによって生じたデータであって、半導体集積回路装置1に供給される電源が一時的に停止した後においても記憶しておくことが必要なデータはフラッシュメモリ2に書き込みがされる。

【0024】

RAM (揮発性メモリ) 4は、随時読み出し/書き込みが可能なメモリであり、入出力データや演算データなどのCPU3などで利用されるユーザデータを一時的に格納する。データ転送ユニット5は、周辺回路8における各レジスタやI/OポートPなどのデータ設定などを行う。

【0025】

割り込みコントローラ6は、CPU3やその他の周辺回路8などからの割り込み処理の制御を行う。BSC 7は、アドレス空間の分割、各種メモリ、周辺デバイスに応じた制御信号の出力を行う。

【0026】

周辺回路8は、たとえば、WDT (Watch Dog Timer) 11、タイマ12

、TPU (Timer Pulse Unit) 13、PPG (Programmable Pulse Generator) 14、SCI (Serial Communication Interface) 15、A/D (Analog/Digital) 変換器 16、および D/A (Digital/Analog) 変換器 17 などから構成されている。

【0027】

WDT 11 は、半導体集積回路装置 1 の暴走などの監視を行う。タイマ 12 は、たとえば、8 ビットのカウンタをベースとしたタイマである。TPU 13 は、PWM (Pulse Width Modulation) 波形を出力することのできるタイマである。

【0028】

PPG 14 は、任意の周期およびパルス幅のパルス出力波形を発生させる。SCI 15 は、外部接続されるデバイスとシリアル通信を行うインタフェースである。A/D 変換器 16 は、アナログ信号をデジタル信号に変換して出力する。D/A 変換器 17 は、デジタル信号をアナログ信号に変換して出力する。

【0029】

クロック発振器 9 は、半導体集積回路装置 1 の動作の基本となるクロック信号を生成し、CPU 3、RAM 4、データ転送ユニット 5、割り込みコントローラ 6、BSC 7、ならびに周辺回路 8 にそれぞれ供給する。

【0030】

ブート ROM (ブートプログラム格納用メモリ) 10 は、フラッシュメモリを制御する制御プログラムをダウンロードするブートプログラムが格納される。ここでは、ダウンロードされる制御プログラムが、たとえば、フラッシュメモリ 2 への書き込み/消去動作を制御するプログラムとするが、該制御プログラムは、フラッシュメモリ 2 への書き込み/消去動作を制御するだけでなく、フラッシュメモリ 2 からの読み出し動作やその他の動作などを制御する機能を有するものであってもよい。

【0031】

I/O ポート P は、データや制御信号などが入出力される外部ポートである。

【0032】

CPU 3、RAM 4、データ転送ユニット 5、BSC 7、およびブート ROM 10 は、内部バス B1 を介して相互に接続されている。BSC 7、および所定の I/O ポート P は、外部バス B2 を介して相互に接続されている。割り込みコントローラ 6、BSC 7、周辺回路 8、ならびに所定の I/O ポート P は、周辺バス B3 を介して相互にそれぞれ接続されている。

【0033】

また、図 2 は、半導体集積回路装置 1 を用いてデータ処理システム 18 を構成した一例を示す構成図である。データ処理システム 18 は、パーソナルコンピュータなどのホスト (情報処理装置) H、および該ホスト H に接続されたディスクドライブ装置 (データ処理装置) DS などから構成されている。

【0034】

ホスト H とディスクドライブ装置 DS は、たとえば、ATAPI (Advanced Technology Attachment Packet Interface) バスを介して双方向に信号伝送可能に接続されている。

【0035】

ディスクドライブ装置 DS は、たとえば、CD や DVD などの光ディスク媒体に記憶されている情報の再生などを行う。このディスクドライブ装置 DS には、光ディスク媒体のドライブ制御などを行う半導体集積回路装置 1、およびフラッシュメモリ 2 が備えられている。

【0036】

フラッシュメモリ 2 は、たとえば、アプリケーションプログラムなどのユーザデータが格納される記憶エリア DR、およびプロテクトエリア (データ領域) PR などを持っており

、半導体集積回路装置1は、該フラッシュメモリ2に格納されたアプリケーションプログラムに基づいて光ディスク媒体のドライブ制御を行う。

【0037】

また、プロテクトエリアPRは、半導体集積回路装置1がフラッシュメモリ2を制御する制御プログラムの転送を中止させるか、否か（若しくは許可させるか）を設定するプロテクトデータが格納される領域である。

【0038】

図3は、半導体集積回路装置1の各動作モードにおけるフラッシュメモリ2の対応を示した図である。

【0039】

図3においては、左側から右側にかけて、動作モード、フラッシュメモリ2のプロテクトエリアPRに格納されたプロテクトデータの値、データバス幅、起動エリア、および制御プログラムダウンロードの可／不可についてそれぞれ示している。

【0040】

図示するように、たとえば、動作モードがブートモードの際には、データバス幅は8ビットとなり、起動はブートプログラムからとなる。このとき、フラッシュメモリ2のプロテクトエリアPRに「ALL H' FF」（たとえば、プロテクトエリアPRの全エリアに「1」のデータが格納されている状態）のプロテクトデータが格納されている場合、制御プログラムのダウンロードは可能（第1の状態）となる。

【0041】

また、プロテクトエリアPRに「ALL H' FF」以外のプロテクトデータが格納されている場合、制御プログラムのダウンロードは不可（第2の状態）となる。プロテクトエリアPRのプロテクトデータが「ALL H' FF」、または「ALL H' FF」以外のいずれでもない場合には不定となり、フラッシュメモリ2の接続（データバス幅）により異なることになる。

【0042】

次に、本実施の形態における半導体集積回路装置を用いたデータ処理システム18の作用について説明する。

【0043】

始めに、ホストHからアプリケーションプログラムなどのユーザデータをフラッシュメモリ2に書き込み、プロテクトデータを設定するまでの動作について、図2、および図4のフローチャートを用いて説明する。

【0044】

ここで、図2においては、動作処理に係わる主要なブロックのみを示しており、図2中に示した▲1▼～▲5▼、および▲1▼'は、動作の流れを示した番号である。

【0045】

まず、リセットが解除され、半導体集積回路装置1がブートモードに遷移し（ステップS101）、CPU3は、ブートROM10からフラッシュメモリ2の制御プログラムをダウンロードするためのブートプログラムを読み出す（▲1▼）。

【0046】

ここで、図5は、半導体集積回路装置1における状態遷移を示す状態遷移図であり、図6は、半導体集積回路装置1の各ポート機能の説明図である。

【0047】

図示するように、半導体集積回路装置1には、リセット端子RESと、通常動作モード、またはブートモードモードを設定するモード端子（ブートモード設定用外部端子）MD0～MD2とが設けられている。

【0048】

たとえば、リセット端子RESに「0」（Lo信号）が入力された際には半導体集積回路装置1がリセット状態となり（状態J1）、モード端子MD1に「0」、モード端子MD2に「1」（Hi信号）が入力された際には該半導体集積回路装置1が通常動作モードと



なる(状態J2)。

【0049】

また、モード端子MD2、0に'0'、モード端子MD1に'1'が入力されると、半導体集積回路装置1はブートモードに遷移する(状態J3)。

【0050】

続いて、図2、図4に示すように、ホストHとのビットレートの合わせ込みを行った後(ステップS102)、CPU3は、フラッシュメモリ2のプロテクトエリアPRに書き込まれているプロテクトデータを参照し(▲1▼)、該プロテクトデータがプロテクト状態となっているか、否かを判断する(ステップS103)。

【0051】

このとき、プロテクトデータがプロテクト状態(第2の状態)となっている際には、半導体集積回路装置1は、スタンバイ状態(あるいは、スリープ状態、無限ループ)となる(ステップS104)。

【0052】

ステップS103の処理において、フラッシュメモリ2のプロテクトデータがプロテクト状態となっていない場合(第1の状態)には、CPU3は、ブートプログラムに基づいて、フラッシュメモリ2の制御プログラム(▲2▼)をホストHからSCI15を介してRAM4にダウンロードする(ステップS105)。

【0053】

そして、CPU3は、RAM4にダウンロードされた制御プログラムに基づいて(ステップS106)、フラッシュメモリ2の書き込み/消去動作を制御する(▲3▼)。

【0054】

そして、ホストからデータ書き込み、あるいはデータ消去のコマンドを受信すると(ステップS107)、半導体集積回路装置1は、フラッシュメモリ2のデータ消去(ステップS108)、または該コマンドに従ってフラッシュメモリ2へのデータ書き込み(ステップS109)を行う。

【0055】

たとえば、ステップS107の処理において、アプリケーションプログラムなどのユーザデータをフラッシュメモリ2に書き込む際には、ホストHから半導体集積回路装置1にデータ書き込みのコマンドが出力される。

【0056】

このコマンドを受け取ると、ホストHからユーザデータ(▲4▼)が半導体集積回路装置1に出力され、SCI15を介してRAM4にダウンロードされる。そして、CPU3は、制御プログラムに基づいて、RAM4にダウンロードされたユーザデータをフラッシュメモリ2の記憶エリアDRに書き込む(▲5▼)。このとき、CPU3は、フラッシュメモリ2のプロテクトエリアPRに、「H'FF」以外の任意の値をプロテクトデータとして書き込む。

【0057】

次回からは、半導体集積回路装置1がブートモードによって起動しても、ステップS103の処理において、プロテクトデータがプロテクト状態となっていると判断するので、半導体集積回路装置1がスタンバイ状態となり、制御プログラムのダウンロードが一切行われないことになる。

【0058】

これにより、フラッシュメモリ2に格納されたユーザデータの再書き込みや消去などが防止されるだけでなく、たとえば、読み出し動作を制御する制御プログラムなどのダウンロードも防止することができるので、第三者などによるユーザデータの読み出しなども防止することができる。

【0059】

また、ブートモード起動時の半導体集積回路装置1とホストHとの通信プロトコルについて、図7を用いて説明する。

## 【0060】

図7においては、上方から下方にかけて、ビットレートの合わせ込み時、制御プログラムの転送時、および制御プログラムの実行時における半導体集積回路装置1、およびホストHの処理動作の流れについてそれぞれ示している。

## 【0061】

まず、ビットレートの合わせ込みを行う場合、ホストHは、所定のビットレートでデータ「H' 00」を半導体集積回路装置1に連続送信する。半導体集積回路装置1は、受信した「H' 00」のLowレベル期間を測定してビットレートを計算し、たとえばRS-232調歩同期シリアル通信のビットレートを設定する。

## 【0062】

ここで、ホストHと半導体集積回路装置1との通信は、RS-232調歩同期シリアル通信以外でもよく、たとえば、USBやイーサネット（登録商標）などを用いて通信することにより、より高速なデータ転送を可能とすることができる。

## 【0063】

その後、半導体集積回路装置1は、ビットレートの設定終了の合図として「H' 00」などの1バイトデータをホストHに送信する。ホストHは、「H' 00」を受信すると、たとえば、「H' 55」などの1バイトデータを半導体集積回路装置1に送信する。

## 【0064】

半導体集積回路装置1は、「H' 55」のデータを受け取ると、フラッシュメモリ2のプロテクトエリアPRに記憶されているプロテクトデータを読み出し、該プロテクトデータが「H' FF」であれば、制御プログラムのダウンロードが可能であることを示す「H' AA」などのデータをホストHに送信する。

## 【0065】

また、半導体集積回路装置1は、プロテクトデータが「H' FF」以外であれば、制御プログラムのダウンロードが不可であることを示す「H' FF」のデータをホストHに送信し、動作を停止（スタンバイ状態など）する。

## 【0066】

次に、制御プログラムの転送時において、ホストHは、転送する制御プログラムのバイト数（N）を上位バイト、下位バイトの順に2バイト送信する。そして、半導体集積回路装置1は、受信した2バイトデータをエコーバックする。

## 【0067】

その後、ホストHは、制御プログラムを1バイト毎に送信する（N回繰り返す）。半導体集積回路装置1は、受信したデータをホストHにエコーバックするとともに、RAM4に転送する（N回繰り返す）。そして、すべてのデータの受信が完了すると、半導体集積回路装置1は、「H' AA」をホストHに送信する。

## 【0068】

続いて、制御プログラムの実行において、半導体集積回路装置1は、RAM4に格納された制御プログラムに基づいてフラッシュメモリ2の書き込み/消去動作の制御を行う。

## 【0069】

それにより、本実施の形態においては、フラッシュメモリ2へのユーザデータの書き込み後にプロテクトデータによってプロテクトをかけることにより、半導体集積回路装置1を用いた該フラッシュメモリ2へのユーザデータの再書き込み/消去/読み出しなどを防止することができる。

## 【0070】

また、本実施の形態においては、プロテクトデータの判断（図4、ステップS103）をビットレートの合わせ込みが終了した後に行っていたが、このプロテクトデータの判断はこれに限定されるものではない。

## 【0071】

たとえば、ビットレートの合わせ込み（図4、ステップS102）の前や、制御プログラムをRAM4にダウンロード（図4、ステップS105）した後など、プロテクトデータ

の判断は、制御プログラムによるフラッシュメモリ2の制御が行われる以前であれば、どのようなタイミングであってもよい。

【0072】

以上、本発明者によってなされた発明を発明の実施の形態に基づき具体的に説明したが、本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。

【0073】

【発明の効果】

本願によって開示される発明のうち、代表的なものによって得られる効果を簡単に説明すれば、以下のとおりである。

【0074】

(1) 不揮発性メモリへのユーザデータの書き込み後に第2の状態となるプロテクトデータを設定することにより、半導体集積回路装置を用いての該不揮発性メモリへのユーザデータの再書き込み/消去/読み出しなどを確実に防止することができる。

【0075】

(2) 上記(1)により、不揮発性メモリを取り外さない限り、該不揮発性メモリに格納されたユーザデータを隠蔽できるので、データ処理システムの信頼性を大幅に向上することができる。

【図面の簡単な説明】

【図1】本発明の一実施の形態による半導体集積回路装置のブロック図である。

【図2】図1の半導体集積回路装置を用いて構成したデータ処理システムのブロック図である。

【図3】図2の半導体集積回路装置の各動作モードに対応するフラッシュメモリの状態説明図である。

【図4】図2のデータ処理システムにおける動作フローチャートである。

【図5】図1の半導体集積回路装置における状態遷移図である。

【図6】図1の半導体集積回路装置における端子機能の説明図である。

【図7】図2のデータ処理システムにおける通信動作処理の流れを示す説明図である。

【符号の説明】

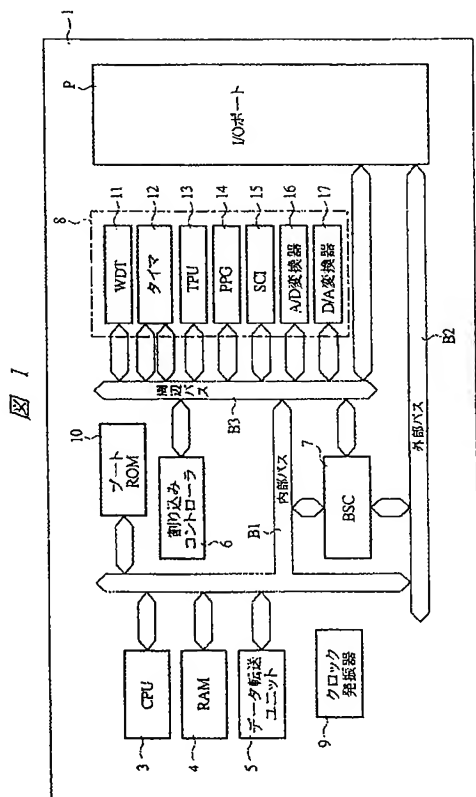
- 1 半導体集積回路装置
- 2 フラッシュメモリ(不揮発性メモリ)
- 3 CPU(制御部)
- 4 RAM(揮発性メモリ)
- 5 データ転送ユニット
- 6 割り込みコントローラ
- 7 BSC
- 8 周辺回路
- 9 クロック発振器
- 10 ブートROM(ブートプログラム格納用メモリ)
- 11 WDT
- 12 タイマ
- 13 TPU
- 14 PPG
- 15 SCI
- 16 A/D変換器
- 17 D/A変換器
- 18 データ処理システム
- H ホスト(情報処理装置)
- DS ディスクドライブ装置(データ処理装置)
- P I/Oポート



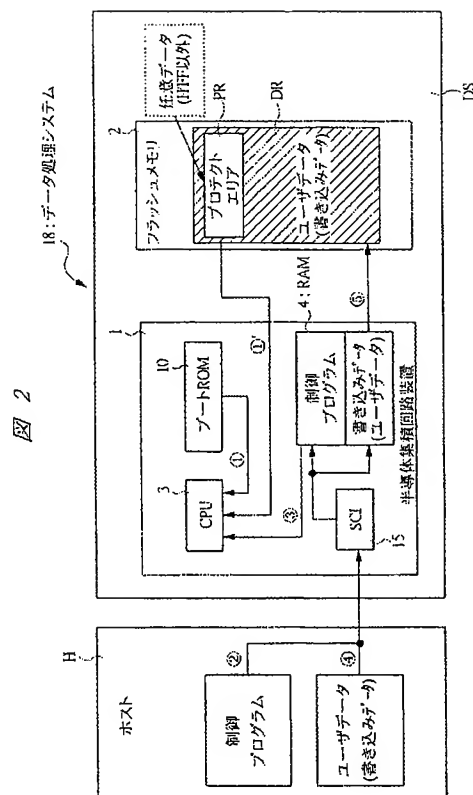
MD0～MD2 モード端子（ブートモード設定用外部端子）

RES リセット端子

【図1】



【図2】



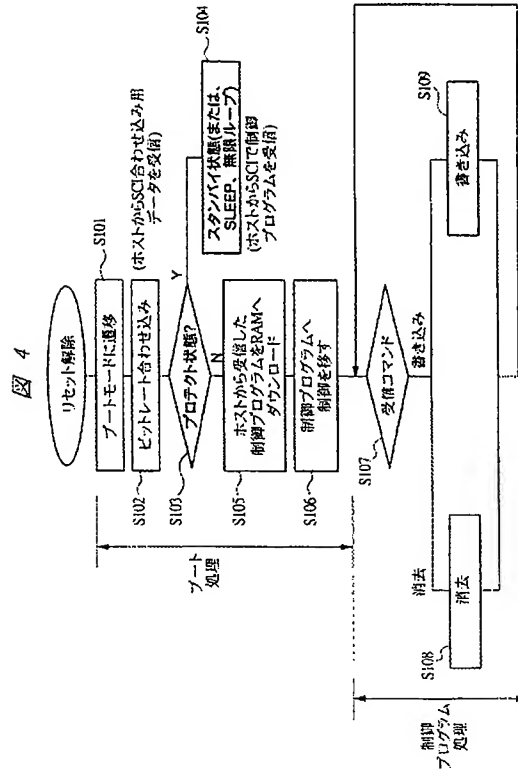


【図3】

図 3

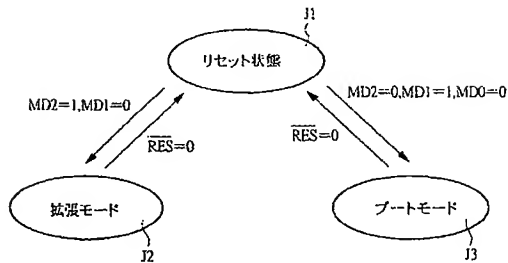
No.	動作モード	フラッシュメモリ上の プロテクトエリアの値	データバス幅	起動エリア	制御プログラム ダウンロードの可/不可
1	拡張モード1	-	8ビット	フラッシュメモリ (ユーザープログラム)	-
2	拡張モード2	-	16ビット	フラッシュメモリ (ユーザープログラム)	-
3	拡張モード3	-	32ビット	フラッシュメモリ (ユーザープログラム)	-
4	ブートモード	ALL H'FF	8ビット	ブートプログラム	可
5		ALL H'FF以外	8ビット	ブートプログラム	不可
6		ALL H'FFまたは、 ALL H'FF以外でない	8ビット	ブートプログラム	不足(メモリ)の接続方法 により異なる。) 不可

【図4】



【図5】

図 5



【図6】

図 6

端子名	入出力	機能
RES	入力	リセット
MD2	入力	動作モードを設定
MD1	入力	動作モードを設定
MD0	入力	動作モードを設定

【図7】

図 7

項目	ホストの動作	半導体集積回路装置の動作
ブートモード起動	所定のビットレートでデータH'00を連続送信	リセットスタート後ブートプログラムへ分岐
ビットレート 合わせ込み	H'00を正常に受信したらH'55を1バイト送信 H'AAを受信	受信データH'00のLow期間を測定 ビットレートを計算し、RS-232Cリアル通信を設定 ビットレート調整終了の合図としてH'00を1バイト送信 H'55を受信 フラッシュメモリ内のプロテクトエリアをリードする プロテクトコードが一致したらホストへH'AAを送信 する(不一致の場合はH'FFを送信し動作を停止)
制御プログラムの 転送	転送する制御プログラムのバイト数(N)を 上位バイト、下位バイトの順に2バイト送信 制御プログラムを1バイト毎に送信(同様に繰り返し)	受信した2バイトのデータをホストへエコーバック 受信したデータをホストにエコーバックすると共に RAMへ転送する(N回繰り返し) 受信完了の合図としてH'AAを送信
制御プログラムの 実行	H'AAを受信	RAMに転送された制御プログラムへ分岐し 実行を開始









(8, 2)

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2004-318330**

(43)Date of publication of application : **11.11.2004**

(51)Int.Cl.

G06F 11/00  
G06F 1/00  
G06F 9/445  
G06F 12/14

(21)Application number : **2003-109170**

(71)Applicant : **RENESAS TECHNOLOGY CORP**

(22)Date of filing : **14.04.2003**

(72)Inventor : **IJIMA MASAHIRO  
ASAI TOSHIO**

## (54) SEMICONDUCTOR INTEGRATED CIRCUIT DEVICE AND DATA PROCESSING SYSTEM

(57)Abstract:

**PROBLEM TO BE SOLVED:** To prevent leakage of user data after writing them in a semiconductor integrated circuit device allowing connection of an external non-volatile memory.

**SOLUTION:** When the semiconductor integrated circuit device 1 is shifted to a boot mode after resetting, a CPU 3 reads a boot program for downloading a control program for a flash memory 2 from a boot ROM 10. Subsequently, matching of a bit rate with a host H is carried out, and the CPU 3 refers protect data written in a protect area PR of the flash memory 2 for determining whether the protect data are in a protected condition. In this process, if the protect data are in the protected condition, the semiconductor circuit device 1 is set to a standby condition (a sleep condition or an endless loop), and consequently, downloading of the control program cannot be executed at all.

